

TORSION POINTS ON HYPERELLIPTIC JACOBIANS VIA ANDERSON'S p -ADIC SOLITON THEORY

YUKEN MIYASAKA AND TAKAO YAMAZAKI

ABSTRACT. We show that torsion points of certain orders are not on a theta divisor in the Jacobian variety of a hyperelliptic curve given by the equation $y^2 = x^{2g+1} + x$ with $g \geq 2$. The proof employs a method of Anderson who proved an analogous result for a cyclic quotient of a Fermat curve of prime degree.

1. INTRODUCTION

Let K be a field of characteristic zero. Let A be an abelian variety over K and Z ($\neq A$) a closed subvariety of A . A celebrated result of Raynaud [11] implies that the intersection of Z with torsion points A_{tor} on A is finite, if Z is a curve of genus at least two, or if A is absolutely simple. However, it is usually not easy to determine this finite set $Z \cap A_{\text{tor}}$ explicitly for given A and Z .

Now let us assume $A = J$ is the Jacobian variety of a smooth projective connected curve X of genus $g \geq 2$. Of particular interest is the case where $Z = X$ is the Abel-Jacobi embedded image of X with respect to some base point. Since Coleman [4] determined the set $X \cap J_{\text{tor}}$ explicitly when X is a Fermat curve, many works have been done in this direction. See [15] for a lucid survey on this subject. Anderson [1] considered the case where $Z = \Theta$ is the theta divisor of J . He proved that torsion points of certain prime orders are not on Θ when X is a cyclic quotient of a Fermat curve of prime degree. For details of this result and its generalization by Grant [6], see Remark 1.3 below. In order to prove his result, Anderson developed a p -adic analogue of the theory of *tau function*, which was originally introduced by Sato [12, 13] (see also [14]) in his study of soliton equations (in the complex analytic setting). In this paper, we apply Anderson's theory to other curves and prove analogous results.

Let us state our main result. Fix an integer $g \geq 2$. Let K be a field of characteristic zero that contains a primitive $4g$ -th root ζ of unity. We consider a hyperelliptic curve X of genus g over K defined by the equation

$$y^2 = x^{2g+1} + x. \tag{1.1}$$

Date: November 13, 2011.

Key words and phrases. Torsion in Jacobian, theta divisor, Sato Grassmannian, p -adic tau function.

The first author is supported by JSPS Research Fellowship for Young Scientists. The second author is supported by Grant-in-Aid for Challenging Exploratory Research (22654001), Grant-in-Aid for Young Scientists (A) (22684001), and Inamori Foundation.

Let ∞ be the K -rational point at which the functions x and y have poles. There is an automorphism r of X of order $4g$ defined by $r(x, y) = (\zeta^2 x, \zeta y)$. Let $G := \langle r \rangle$ be the subgroup of $\text{Aut}(X)$ generated by r . The Jacobian variety J of X will be considered as a $\mathbb{Z}[G]$ -module by the induced action of G . (We will see in §3.8 that J is absolutely simple when $g > 45$.) We define the theta divisor Θ to be the set of $\mathcal{L} \in J$ such that $H^0(X, \mathcal{L}((g-1)\infty)) \neq \{0\}$.

Let p be a prime number such that $p \equiv 1 \pmod{4g}$, and choose a prime ideal $\wp \subset \mathbb{Z}[\zeta]$ lying above p . We write χ for the composition of

$$G \rightarrow \mathbb{Z}[\zeta]^* \twoheadrightarrow (\mathbb{Z}[\zeta]/\wp)^* = \mathbb{F}_p^*$$

where the first map is defined by $r \mapsto \zeta$. We will show in Lemma 4.1 below that, for $i = 0, 1, \dots, 4g-1$, we have

$$\dim_{\mathbb{F}_p} J[p]^{\chi^i} = \begin{cases} 0 & (i : \text{even}) \\ 1 & (i : \text{odd}), \end{cases}$$

where $J[p]^{\chi^i} = \{\mathcal{L} \in J[p] \mid r^* \mathcal{L} = \chi^i(r) \mathcal{L}\}$. Our main results are the following:

Theorem 1.1. *If $i \in \{1, 3, \dots, 4g-1\}$ is relatively prime to $4g$, then we have*

$$(J[p]^{\chi^i} + J[2]) \cap \Theta \subseteq J[2].$$

Theorem 1.2. *Assume that K is a finite extension of \mathbb{Q}_p . Let $Q \in X(K)$ and put $\mathcal{L}_Q := \mathcal{O}_X(Q - \infty)$. Assume that the coordinates $x(Q)$ and $y(Q)$ of Q belong to the integer ring of K . If $i \in \{1, 3, \dots, 4g-1\}$ is relatively prime to $4g$, then we have*

$$(J[p]^{\chi^i} + \mathcal{L}_Q) \cap \Theta = \{\mathcal{L}_Q\}.$$

Note that the set $\Theta \cap J_{\text{tor}}$ is explicitly determined when $g = 2$ by Boxall-Grant [3]. It consists of twenty-two points (over an algebraically closed field).

Remark 1.3. For the sake of comparison, we recall Anderson's result [1]. Fix an odd prime number l , integers $a \geq b > 1$ such that $l+1 = a+b$, and a primitive l -th root ζ_l of unity. Let X be the smooth projective curve defined by $y^l = x^a(1-x)^b$, and define J and Θ similarly as above. (By Koblitz-Rohrlich [7], J is absolutely simple.) There is an automorphism γ of X defined by $\gamma(x, y) = (x, \zeta_l y)$, which induces a $\mathbb{Z}[\zeta_l]$ -module structure on J such that ζ_l acts by γ^* . For an ideal \mathfrak{a} of $\mathbb{Z}[\zeta_l]$, we write $J[\mathfrak{a}]$ for the \mathfrak{a} -torsion subgroup of J . Let p be a prime number such that $p \equiv 1 \pmod{l}$ and take a prime ideal \wp over p . Anderson's result [1, Theorem 1] is the following:

$$(J[\wp] + J[(1-\zeta_l)]) \cap \Theta \subseteq J[(1-\zeta_l)].$$

Grant [6] improved Anderson's result by showing for all $n \geq 1$

$$(J[\wp^n] + J[(1-\zeta_l)]) \cap \Theta \subseteq J[(1-\zeta_l)]$$

under the assumption that X is hyperelliptic (that happens iff $a \in \{2, (l+1)/2, l-1\}$).

This paper is organized as follows. In §2 we recall some results from Anderson [1]. In §3 we study geometry of the hyperelliptic curve (1.1). The proof of Theorems 1.1 and 1.2 is completed in §4. The last section §5 is devoted to an illustration of Anderson's results recalled in §2.

2. REVIEW OF ANDERSON'S THEORY

In this section, we recall (bare minimum of) results of Anderson [1, §2, 3]. We formulate all results without any use of Sato Grassmannian (which is actually central in Anderson's theory). All results in this section are merely reformulation of loc. cit., but for the completeness sake we include some explanation using Sato Grassmannian in §5.

2.1. Krichever pairs. Let X be a smooth projective geometrically irreducible curve over a field K equipped with a K -rational point ∞ . We fix an isomorphism $N_0 : \hat{\mathcal{O}}_{X,\infty} \cong K[[T^{-1}]]$, and write N for the composition map $\text{Spec } K((T^{-1})) \rightarrow \text{Spec } K[[T^{-1}]] \xrightarrow{N_0} X$. (Here $K[[T^{-1}]]$ is the ring of power series in T^{-1} with coefficients in K , and $K((T^{-1}))$ is its fraction field.) An N -trivialization of a line bundle \mathcal{L} on X is an isomorphism $\sigma : N^*\mathcal{L} \cong K((T^{-1}))$ of $K((T^{-1}))$ -vector spaces induced by an isomorphism $\sigma_0 : N_0^*\mathcal{L} \cong K[[T^{-1}]]$ of $K[[T^{-1}]]$ -modules. A pair (\mathcal{L}, σ) of a line bundle \mathcal{L} on X and an N -trivialization σ of \mathcal{L} is called a *Krichever pair*. Two Krichever pairs are said to be isomorphic if there exists an isomorphism of line bundles compatible with N -trivializations. We write $\text{Kr}(X, N)$ for the set of isomorphism classes of Krichever pairs. We have a canonical surjective map

$$[\cdot] : \text{Kr}(X, N) \rightarrow \text{Pic}(X), \quad [(\mathcal{L}, \sigma)] = \mathcal{L}.$$

For each $n \in \mathbb{Z}$ we define $\text{Kr}^n(X, N) := \{(\mathcal{L}, \sigma) \in \text{Kr}(X, N) \mid \deg(\mathcal{L}) = n\}$ to be the inverse image of $\text{Pic}^n(X)$ by $[\cdot]$.

2.2. A Krichever pair associated to a Weil divisor. Let $D = \sum_{P \in X} n_P P$ be a Weil divisor on X . The associated line bundle $\mathcal{O}_X(D)$ admits an N -trivialization $\sigma(D)$ induced by the composition $\mathcal{O}_X(D) \hookrightarrow K(X) \xrightarrow{N} K((T^{-1})) \xrightarrow{T^{-n_\infty}} K((T^{-1}))$. (Here n_∞ is the coefficient of ∞ in D .) Thus we obtain a Krichever pair $(\mathcal{O}_X(D), \sigma(D))$.

2.3. Vector space associated to a Krichever pair. For $(\mathcal{L}, \sigma) \in \text{Kr}(X, N)$, we define a K -subspace $W(\mathcal{L}, \sigma)$ of $K((T^{-1}))$ by

$$W(\mathcal{L}, \sigma) := \{\sigma N^* f \in K((T^{-1})) \mid f \in H^0(X \setminus \{\infty\}, \mathcal{L})\}.$$

Note that $A := W(\mathcal{O}_X, N)$ is a K -subalgebra of $K((T^{-1}))$ such that $\text{Spec } A \cong X \setminus \{\infty\}$, and that $W(\mathcal{L}, \sigma)$ is a A -submodule of $K((T^{-1}))$ for any $(\mathcal{L}, \sigma) \in \text{Kr}(X, N)$. The following fact is fundamental to us. (See Proposition 5.1 for details.)

Proposition 2.1. *Let $(\mathcal{L}, \sigma), (\mathcal{L}', \sigma') \in \text{Kr}(X, N)$. If $W(\mathcal{L}, \sigma) = W(\mathcal{L}', \sigma')$, then we have $(\mathcal{L}, \sigma) = (\mathcal{L}', \sigma')$.*

2.4. Admissible basis. Let $(\mathcal{L}, \sigma) \in \text{Kr}(X, N)$. Put $W = W(\mathcal{L}, \sigma)$ and $i_0 := \deg(\mathcal{L}) + 1 - g$. It follows from the Riemann-Roch theorem that there is a K -basis $\{w_i\}_{i=1}^\infty$ of W such that

- (1) $\{\deg w_i\}_{i=1}^\infty$ is a strictly increasing sequence,
- (2) w_i is monic for all i , and
- (3) $\deg(w_i - T^{i-i_0})$ is a bounded function of i .

(Here $\deg : K((T^{-1}))^* \rightarrow \mathbb{Z}$ is the sign inversion of the normalized valuation, and $w \in K((T^{-1}))$ is called monic iff $\deg(w - T^{\deg w}) < \deg(w)$.) Such a K -basis $\{w_i\}_{i=1}^\infty$ of W will be called *admissible*. We call $i(W) := i_0$ the *index* of W . (The integer i_0 can be read off from W , as it is the only integer that satisfies the property (3) above.) The *partition* $\kappa = (\kappa_i)_{i=1}^\infty$ of W is a non-increasing sequence of non-negative integers defined by

$$\kappa_i := i - i(W) - \deg(w_i),$$

which satisfies $\kappa_i = 0$ for sufficiently large i . The partition κ does not depend on a choice of an admissible basis. (Actually, it depends only on \mathcal{L} .) The integer $\ell(\kappa) := \max\{i \mid \kappa_i \neq 0\}$ will be called the *length* of the partition κ .

2.5. Group structure. We regard $\text{Kr}(X, N)$ as an abelian group by the tensor product, so that the identity element is given by (\mathcal{O}_X, N) . Note that $[\cdot] : \text{Kr}(X, N) \rightarrow \text{Pic}(X)$ is a group homomorphism. Take $(\mathcal{L}, \sigma), (\mathcal{L}', \sigma') \in \text{Kr}(X, N)$ and let $(\mathcal{L}'', \sigma'') = (\mathcal{L} \otimes \mathcal{L}', \sigma \otimes \sigma')$ be their product. Then $W(\mathcal{L}'', \sigma'')$ coincides with the K -subspace of $K((T^{-1}))$ spanned by $\{ww' \in K((T^{-1})) \mid w \in W(\mathcal{L}, \sigma), w' \in W(\mathcal{L}', \sigma')\}$.

2.6. Theta divisor. Let us write $J := \text{Pic}^0(X)$ for the *Jacobian variety* of X . Let us also write $\Theta \subset J$ for the *theta divisor*, which is defined to be the set of $\mathcal{L} \in J$ such that $H^0(C, \mathcal{L}((g-1)\infty)) \neq \{0\}$. Observe that $(\mathcal{L}, \sigma) \in \text{Kr}^0(X, N)$ satisfies $\mathcal{L} \in \Theta$ if and only if

$$W(\mathcal{L}, \sigma) \cap T^{g-1}K[[T^{-1}]] \neq \{0\},$$

because there is an isomorphism $W(\mathcal{L}, \sigma) \cap T^{g-1}K[[T^{-1}]] \cong H^0(X, \mathcal{L}((g-1)\infty))$.

2.7. Automorphism of a curve. Suppose we are given two endomorphisms r and \bar{r} of K -schemes which fit in the commutative diagram

$$\begin{array}{ccc} \text{Spec } K((T^{-1})) & \xrightarrow{N} & X \\ \bar{r} \downarrow & & \downarrow r \\ \text{Spec } K((T^{-1})) & \xrightarrow{N} & X. \end{array}$$

Assume further that $r(\infty) = \infty$. Then, for $(\mathcal{L}, \sigma) \in \text{Kr}(X, N)$, the composition

$$(r, \bar{r})^* \sigma : N^* r^* \mathcal{L} \cong \bar{r}^* N^* \mathcal{L} \xrightarrow{\bar{r}^* \sigma} \bar{r}^* K((T^{-1})) \cong K((T^{-1}))$$

is an N -trivialization of $r^*\mathcal{L}$. Therefore we get an induced homomorphism

$$\mathrm{Kr}(X, N) \rightarrow \mathrm{Kr}(X, N), \quad (\mathcal{L}, \sigma) \mapsto (r^*\mathcal{L}, (r, \bar{r})^*\sigma),$$

which, by abuse of notation, will be denoted by r^* . This homomorphism is compatible with $[\cdot]$ in the sense that $[r^*(\mathcal{L}, \sigma)] = r^*\mathcal{L}$.

2.8. The p -adic analytic part of Krichever pairs. From now on, we assume p is a prime number and K is a finite extension of the field \mathbb{Q}_p of p -adic numbers. Let $|\cdot|$ the absolute value on K such that $|p| = p^{-1}$. Let $H(K)$ be the ring defined by

$$H(K) := \left\{ \sum_{i=-\infty}^{\infty} a_i T^i \mid a_i \in K, \sup_{i=-\infty}^{\infty} |a_i| < \infty, \lim_{i \rightarrow \infty} |a_i| = 0 \right\}.$$

Note that $H(K)$ is equipped with the norm

$$\left\| \sum_i a_i T^i \right\| := \sup_i |a_i|,$$

and $(H(K), \|\cdot\|)$ is a p -adic Banach algebra over K .

We write $\mathrm{Kr}_{\mathrm{an}}(X, N)$ for the subset of $\mathrm{Kr}(X, N)$ consisting of all Krichever pairs (\mathcal{L}, σ) such that $W(\mathcal{L}, \sigma)$ admits an admissible basis $\{w_i\}$ satisfying

- (1) $w_i \in H(K)$ for all i , and
- (2) $\|w_i\| = 1$ for almost all i .

For each $n \in \mathbb{Z}$, we put $\mathrm{Kr}_{\mathrm{an}}^n(X, N) = \mathrm{Kr}_{\mathrm{an}}(X, N) \cap \mathrm{Kr}^n(X, N)$.

For $(\mathcal{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we write $\bar{W}(\mathcal{L}, \sigma)$ for the closure of $W(\mathcal{L}, \sigma)$ in $H(K)$. One recovers $W(\mathcal{L}, \sigma)$ from $\bar{W}(\mathcal{L}, \sigma)$ by $W(\mathcal{L}, \sigma) = \bar{W}(\mathcal{L}, \sigma) \cap K((T^{-1}))$. (Here we regard both $H(K)$ and $K((T^{-1}))$ as K -vector subspaces of $\prod_{i \in \mathbb{Z}} K T^i$.) Hence the following proposition is a consequence of Proposition 2.1.

Proposition 2.2. *Let $(\mathcal{L}, \sigma), (\mathcal{L}', \sigma') \in \mathrm{Kr}_{\mathrm{an}}(X, N)$. If $\bar{W}(\mathcal{L}, \sigma) = \bar{W}(\mathcal{L}', \sigma')$, then we have $(\mathcal{L}, \sigma) = (\mathcal{L}', \sigma')$.*

2.9. The p -adic loop group. We define the p -adic loop group $\Gamma(K)$ to be the subgroup of $H(K)^\times$ consisting of all $\sum_i h_i T^i \in H(K)^\times$ such that $|h_0| = 1$, $|h_i| \leq 1$ for all $i \leq 0$, and there exists a real number $0 < \rho < 1$ such that

$$|h_i| \leq \rho^i \quad \text{for all } i \geq 1.$$

Define the subgroups $\Gamma_+(K)$ and $\Gamma_-(K)$ of $\Gamma(K)$ by

$$\begin{aligned} \Gamma_+(K) &:= \left\{ \sum_i h_i T^i \in \Gamma(K) \mid h_0 = 1, h_i = 0 \ (i < 0) \right\}, \\ \Gamma_-(K) &:= \left\{ \sum_i h_i T^i \in \Gamma(K) \mid h_i = 0 \ (i > 0) \right\}. \end{aligned}$$

Proposition 2.3 ([1, §3.3]; see also §5.3 below). *There is an action of $\Gamma(K)$ on $\mathrm{Kr}_{\mathrm{an}}(X, N)$ characterized by the following property: for any $h \in \Gamma(K)$ and $(\mathcal{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $\bar{W}(h(\mathcal{L}, \sigma)) = h\bar{W}(\mathcal{L}, \sigma)$. (Here the right hand side means $\{hw \mid w \in \bar{W}(\mathcal{L}, \sigma)\}$.) Moreover, this action satisfies the following properties:*

- (1) *For any $h \in \Gamma(K)$ and $(\mathcal{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $\deg[h(\mathcal{L}, \sigma)] = \deg[(\mathcal{L}, \sigma)]$.*
- (2) *For any $h \in \Gamma_-(K)$ and $(\mathcal{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $[h(\mathcal{L}, \sigma)] = [(\mathcal{L}, \sigma)]$.*
- (3) *Suppose $(\mathcal{O}_X, N) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$. For any $h \in \bar{W}(\mathcal{O}_X, N) \cap \Gamma(K)$ and $(\mathcal{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}(X, N)$, we have $[h(\mathcal{L}, \sigma)] = [(\mathcal{L}, \sigma)]$.*

2.10. Dwork loops and Anderson's theorem. In his study of the p -adic properties of zeta functions of hypersurfaces over finite fields (see, for example, [5]), Dwork constructed a special element of $\Gamma(K)$ (which we call a Dwork loop). We shall exploit his construction. Assume that K contains a $(p-1)$ -st root π of $-p$. Let u be a unit of the integer ring of K . A *Dwork loop* is defined by

$$h(T) := \exp(\pi((uT) - (uT)^p)).$$

For all $i \geq 0$, we have (see, for example [8, Chapter I])

$$|h_i| \leq |p|^{i(p-1)/p^2},$$

where $h(T) = \sum_i h_i T^i$. Therefore $h(T) \in \Gamma_+(K)$.

The following theorem is technically crucial in Anderson [1]; see §5.3 for details.

Theorem 2.4 ([1, Lemma 3.5.1]). *Assume that $p \geq 7$. Let h be a Dwork loop and $(\mathcal{L}, \sigma) \in \mathrm{Kr}_{\mathrm{an}}^0(X, N)$. We write $\kappa = (\kappa_i)_{i=1}^\infty$ and $\ell(\kappa)$ for the partition of $W(\mathcal{L}, \sigma)$ and the length of κ . Assume further $W(\mathcal{L}, \sigma)$ satisfies that*

- (A1) *there exists an admissible basis $\{w_i\}_{i=1}^\infty$ such that $w_i \in H(K)$ and $\|w_i\| = 1$ for all $i \geq 1$,*
- (A2) *the partition κ satisfies $\max\{\kappa_1, \ell(\kappa)\} < p/4$.*

Then, we have $W(h(\mathcal{L}, \sigma)) \cap T^{g-1}K[[T^{-1}]] = \{0\}$. Equivalently, we have

$$[h(\mathcal{L}, \sigma)] \notin \Theta.$$

3. GEOMETRY OF A HYPERELLIPTIC CURVE

3.1. A hyperelliptic curve. Let $g > 1$ be an integer. Let K be a field of characteristic zero, and assume that K contains a primitive $4g$ -th root ζ of unity. Let X be the hyperelliptic curve given by the equation (1.1):

$$y^2 = x^{2g+1} + x.$$

There is an automorphism r of X of order $4g$ given by $r(x, y) = (\zeta^2 x, \zeta y)$. Let $G := \langle r \rangle \cong \mathbb{Z}/4g\mathbb{Z}$ be the subgroup of $\mathrm{Aut}(X)$ generated by r . Note that $r(\infty) = \infty$, where $\infty \in X(K)$ is the point at which the functions x and y have poles.

3.2. Singular homology. In this subsection we assume K is a subfield of \mathbb{C} . The singular homology $H_1(X(\mathbb{C}), \mathbb{Z})$ is a free \mathbb{Z} -module of rank $2g$ on which G acts linearly. Let $\rho : G \rightarrow \text{Aut}(H_1(X(\mathbb{C}), \mathbb{Z}))$ be the corresponding representation. Let $\chi : G \rightarrow \mu_{4g}$ be the character given by $\chi(r) = \zeta$.

Lemma 3.1. *The representation $\rho \otimes \mathbb{C}$ is equivalent to $\bigoplus_{i=1,3,\dots,4g-1} \chi^i$. In particular, the minimal polynomial of $\rho(r)$ is $F(X) := X^{2g} + 1$.*

Proof. We consider a $\mathbb{C}[G]$ -module $V = H^0(X, \Omega_{X/\mathbb{C}}^1) = \langle w_i = x^{i-1} dx/y \mid i = 1, \dots, g \rangle_{\mathbb{C}}$. A direct computation shows $r^*(w_i) = \zeta^{2i-1} w_i$. The lemma follows from an isomorphism

$$H_1(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C} \cong V \oplus \text{Hom}(V, \mathbb{C})$$

of $\mathbb{C}[G]$ -modules. □

3.3. Good trivialization. The following is an easy consequence of Hensel's lemma:

Lemma 3.2. *There exists a unique element $u(T) \in 1 + T^{-1}\mathbb{Z}[[T^{-1}]]$ such that*

$$u(T)^{2g} - u(T)^{2g-1} + (T^{-1})^{4g} = 0.$$

We define two elements $x(T), y(T) \in \mathbb{Z}[[T^{-1}]][[T]]$ by

$$x(T) := T^2 u(T), \quad y(T) := -Tx(T)^g.$$

Note that $x(T) \equiv T^2 \pmod{T\mathbb{Z}[[T^{-1}]}}$ and $y(T) \equiv -T^{2g+1} \pmod{T^{2g}\mathbb{Z}[[T^{-1}]}}$. It follows from Lemma 3.2 that $(T^{-2}x(T))^{2g} - (T^{-2}x(T))^{2g-1} + (T^{-1})^{4g} = 0$. By multiplying $T^{4g}x(T)$, we get

$$y(T)^2 = x(T)^{2g+1} + x(T).$$

Therefore we can define an injection $K(X) \hookrightarrow K((T^{-1}))$ of K -algebras by associating x and y with $x(T)$ and $y(T)$ respectively. This induces an isomorphism $N_0 : \hat{\mathcal{O}}_{X,\infty} \cong K[[T^{-1}]]$, and we can apply the results of §2. Note that $A := W(\mathcal{O}_X, N)$ is the K -subalgebra of $K((T^{-1}))$ generated by $x(T)$ and $y(T)$.

3.4. Admissible basis of A . We construct a basis $\{w_i\}$ of A such that

- (1) $w_i \in \mathbb{Z}[[T^{-1}]][[T]]$ for all i ,
- (2) $w_i - T^{2i-2} \in T^{2i-3}\mathbb{Z}[[T^{-1}]]$ for all $i \leq g+1$, and
- (3) $w_i - T^{i-1+g} \in T^{2g}\mathbb{Z}[[T^{-1}]]$ for all $i \geq g+2$.

In particular, $\{w_i\}$ is admissible in the sense of §2.4. First we put

$$u_i = \begin{cases} x(T)^{i-1} & (1 \leq i \leq g), \\ x(T)^{g+(i-g-1)/2} & (i > g, i \not\equiv g \pmod{2}), \\ -y(T)x(T)^{(i-g-2)/2} & (i > g, i \equiv g \pmod{2}). \end{cases}$$

Note that $u_i \in \mathbb{Z}[[T^{-1}]][[T]]$ for all i and $\{u_i\}$ is a K -basis of A . We set $w_i = u_i$ for $i \leq g+1$. Suppose we have constructed w_1, \dots, w_{i-1} for some $i \geq g+2$. There exists

$\delta \in \langle w_1, \dots, w_{i-1} \rangle_{\mathbb{Z}}$ such that $u_i - T^{i-1+g} - \delta \in T^{2g}\mathbb{Z}[[T^{-1}]]$. We then set $w_i := u_i - \delta$. Note that the partition of A is

$$(g, g-1, \dots, 2, 1, 0, 0, \dots),$$

and its length is g .

3.5. Two-torsion points. For any $\mathcal{L} \in J[2]$, we shall construct an N -trivialization σ of \mathcal{L} such that $W(\mathcal{L}, \sigma)$ admits an admissible basis $\{w_i\}$ satisfying $w_i \in \mathbb{Z}[[T^{-1}]][T]$ for all i .

Recall that the Weierstrass points on X are

$$\infty, P_0 = (0, 0), \text{ and } P_i = (\zeta^{2i-1}, 0) \quad (1 \leq i \leq 2g).$$

It is proved in [10, Chapter III, §2] that the two-torsion subgroup $J[2]$ of J consists of line bundles associated to Weil divisors

$$D_I := \sum_{i \in I} (P_i - \infty), \quad I \subset \{0, 1, \dots, 2g\}, \quad |I| \leq g.$$

For a subset $I \subset \{0, 1, \dots, 2g\}$ such that $s := |I| \leq g$, we get a Krichever pair $(\mathcal{L}_I, \sigma_I) := (\mathcal{O}_X(D_I), \sigma(D_I))$ by the construction in §2.2. We further set $L_I := W(\mathcal{L}_I, \sigma_I)$.

We construct a basis $\{w_{I,i}\}_{i=1}^{\infty}$ of L_I as follows: define an element f_I of $H^0(X \setminus \{\infty\}, \mathcal{L}_I) \subset K(x, y)$ by

$$f_I := y \prod_{j \in I} (x - x(P_j))^{-1}.$$

Note that the divisor of f_I satisfies

$$\operatorname{div}(f_I) = \sum_{j \notin I} P_j - \sum_{j \in I} P_j - (2g - 2s + 1)\infty.$$

Now we define for $1 \leq i \leq g - s$,

$$u_{I,i} := T^s x(T)^{i-1}$$

and for $1 \leq i$,

$$u_{I,g-s+i} = \begin{cases} T^s x(T)^{g-s+(i-1)/2} & (i : \text{odd}) \\ T^s f_I(T) x(T)^{(i-2)/2} & (i : \text{even}), \end{cases}$$

where $f_I(T)$ is the image of f_I by the embedding $N^* : K(x, y) \hookrightarrow K((T^{-1}))$. One sees that

$$\deg(u_{I,i}) = \begin{cases} 2i - 2 + s & (1 \leq i \leq g - s) \\ i + g - 1 & (g - s < i). \end{cases}$$

Therefore $\{u_{I,i}\}_{i=1}^{\infty}$ is a K -basis of L_I such that $u_{I,i} \in \mathbb{Z}[[T^{-1}]][T]$ for all i . Now we can produce an admissible basis $\{w_{I,i}\}$ of L_I with required properties by the same procedure as §3.4. Note that the partition of L_I is

$$(g - s, g - s - 1, \dots, 2, 1, 0, 0, \dots),$$

and the length of the partition is $g - s$.

3.6. Points of degree one. We fix a non-Weierstrass point $Q \in X(K)$. Let $(\mathcal{L}_Q, \sigma_Q)$ be the Krichever pair associated to the Weil divisor $Q - \infty$ under the construction in §2.2. We are going to construct an admissible basis $\{w_{Q,i}\}$ of $L_Q := W(\mathcal{L}_Q, \sigma_Q)$ satisfying $w_{Q,i} \in \mathbb{Z}[x(Q), y(Q)][[T^{-1}]] [T]$ for all i .

We define a function $f_Q \in H^0(X \setminus \{\infty\}, \mathcal{L}_Q) \subset K(x, y)$:

$$f_Q := l_Q \cdot (x - x(Q))^{-1}, \quad l_Q := y - x + y(Q) + x(Q).$$

A straightforward computation shows that $\text{div}(f_Q) + Q + (2g - 1)\infty$ is an effective divisor of degree $2g$. We construct a basis $\{u_{Q,i}\}_{i=1}^{\infty}$ of L_Q as follows: for $1 \leq i \leq g$,

$$u_{Q,i} := Tx(T)^{i-1}$$

for $1 \leq i$,

$$u_{Q,g+i} := \begin{cases} Tf_Q(T)x(T)^{(i-1)/2} & (i : \text{odd}) \\ Tx(T)^{g+(i-2)/2} & (i : \text{even}), \end{cases}$$

where $f_Q(T)$ is the image of f_Q in $K((T^{-1}))$ by the embedding N^* . One sees that

$$\deg(u_{Q,i}) = \begin{cases} 2i - 1 & (1 \leq i \leq g) \\ i + g - 1 & (g < i). \end{cases}$$

Therefore $\{u_{Q,i}\}_{i=1}^{\infty}$ is a K -basis of L_Q such that $u_{Q,i} \in \mathbb{Z}[x(Q), y(Q)][[T^{-1}]] [T]$ for all i . Now we can produce an admissible basis $\{w_{Q,i}\}$ of L_Q with required properties by the same procedure as §3.4. Note that the partition of L_Q is

$$(g - 1, g - 2, \dots, 1, 0, 0, \dots),$$

and its length is $g - 1$.

3.7. Action of G on $\text{Kr}(X, N)$. We define a K -algebra automorphism \bar{r} on $K((T^{-1}))$ by

$$\bar{r} \left(\sum_i a_i T^i \right) := \sum_i a_i (\zeta T)^i.$$

Then the diagram

$$\begin{array}{ccc} \text{Spec } K((T^{-1})) & \xrightarrow{N} & X \\ \bar{r} \downarrow & & \downarrow r \\ \text{Spec } K((T^{-1})) & \xrightarrow{N} & X. \end{array}$$

commutes. By §2.7, we get an induced action of G on $\text{Kr}(X, N)$. It holds that $W(r(\mathcal{L}, \sigma)) = \bar{r}(W(\mathcal{L}, \sigma)) (= \{\bar{r}(w) \mid w \in W(\mathcal{L}, \sigma)\})$.

3.8. Remark on the simplicity of Jacobian.¹ (The result of this subsection will not be used in the sequel.) We suppose K is an algebraically closed field. We deduce from a result of Aoki [2] that the Jacobian variety of X is simple as an abelian variety, at least when $g > 45$. To see this, let C' be a smooth projective curve over K defined by $s^{4g} = t(1-t)$. There exists a degree two map $\pi : C' \rightarrow C$ given by $(s, t) \mapsto (c^2 t^2, c(2s-1)t)$, where $c = (-4)^{1/4g}$. Aoki's result [2] shows that the Jacobian variety of C' has exactly two simple factors, provided $g > 45$. The existence of π shows that the Jacobian variety of X must be one of two simple factors.

4. PROOF OF MAIN THEOREM

We keep the notation and assumption in §3. Let p be a prime number such that

$$p \equiv 1 \pmod{4g}.$$

We further assume that K is a finite extension of \mathbb{Q}_p that contains $(p-1)$ -st roots of all integers. Note that $\zeta \in K$.

4.1. p -torsion of the Jacobian. We fix an embedding $\mathbb{Q}(\zeta) \subset \mathbb{Q}_p$, so that we get a prime ideal $\wp := \mathbb{Z}[\zeta] \cap p\mathbb{Z}_p$ of $\mathbb{Z}[\zeta]$ over p . Note that \mathbb{F}_p contains all the $4g$ -th roots of unity. Put $\bar{\zeta} := \zeta \pmod{\wp} \in \mathbb{F}_p$. Let J be the Jacobian variety of X and $J[p]$ the p -torsion subgroup of J . Choosing an embedding $K \subset \mathbb{C}$, we get an isomorphism $J[p] \cong H_1(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{F}_p$. The representation $\rho_p : G \rightarrow \text{Aut}(J[p])$ is thus equivalent to $\rho \otimes \mathbb{F}_p$. Therefore Lemma 3.1 implies the following:

Lemma 4.1. *The minimal polynomial of $\rho_p(r)$ is*

$$F(X) \pmod{p} = \prod_{i=1,3,\dots,4g-1} (X - \bar{\zeta}^i).$$

Consequently, we have

$$J[p] = \bigoplus_{i=1,3,\dots,4g-1} J[p]^{\chi^i}, \quad \dim_{\mathbb{F}_p} J[p]^{\chi^i} = 1 \quad (i = 1, 3, \dots, 4g-1).$$

Here, by abuse of notation, we write χ^i for the composition $G \xrightarrow{\chi^i} \mu_{4g} \hookrightarrow \mathbb{Z}_p^* \xrightarrow{\text{mod } p} \mathbb{F}_p^*$.

Remark 4.2. If we take a different choice for the embedding $\mathbb{Q}(\zeta) \subset \mathbb{Q}_p$, then the characters χ^i are replaced by χ^{ij} for some $j \in (\mathbb{Z}/4g\mathbb{Z})^\times$. By using all such embeddings, proofs of Theorems 1.1 and 1.2 are reduced to the case $i = 1$.

¹This remark is communicated to us by Noriyuki Otsubo.

4.2. An auxiliary lemma.

Lemma 4.3. *We have an equation*

$$T^p - e_0 T = a(T) + g(T) \quad (4.1)$$

for some $e_0 \in \mathbb{Z}_{(p)}^*$, $a(T) \in A \cap \mathbb{Z}[[T^{-1}]][[T]]$ and $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$.

Proof. Setting $p = 4gp' + 1$, we write

$$x^{2gp'}(1 + x^{-2g})^{2gp'} = e_+(x) + e_0 + e_-(x)$$

where $e_{\pm}(x) \in x^{\pm 2g}\mathbb{Z}[x^{\pm 2g}]$ and $e_0 \in \mathbb{Z}$. Note that $e_0 = \binom{2gp'}{p'}$ is a p -adic unit. We compute

$$\begin{aligned} e_+(x) + e_0 + e_-(x) &= x^{2gp'}(1 + x^{-2g})^{2gp'} = (x + x^{1-2g})^{2gp'} \\ &= \left(\frac{x^{2g+1} + x}{x^{2g}} \right)^{2gp'} = \left(\frac{y^2}{x^{2g}} \right)^{2gp'} = \left(\frac{-y}{x^g} \right)^{p-1}. \end{aligned}$$

Recalling $y(T) = -Tx(T)^g$, we get an equation in $K((T^{-1}))$

$$T^p - e_0 T = a(T) + g(T)$$

where $a(T) := -y(T)e_+(x(T))/x(T)^g$ and $g(T) := Te_-(x(T))$. Observe that $a(T)$ is in the image of $A = K[x, y]$ in $K((T^{-1}))$ (since $e_+(x) \in x^{2g}\mathbb{Z}[x]$) and that $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$. \square

4.3. Decomposition of a Dwork loop. The result of §3.4 shows that $(\mathcal{O}_X, N) \in \text{Kr}_{\text{an}}(X, N)$. Recall that $\bar{A} := \bar{W}(\mathcal{O}_X, N)$ is the closure of $A = W(\mathcal{O}_X, N)$ in $H(K)$. Let π and ε_0 be $(p-1)$ -st roots of $-p$ and $1/e_0$ respectively, where $e_0 \in \mathbb{Z}_{(p)}^*$ is the number appearing in Lemma 4.3. (They belong to K by the assumption made at the beginning of this section.) For $0 \leq i \leq p-2$, we define a Dwork loop

$$\begin{aligned} h^{(i)}(T) &:= \exp(\pi((\zeta_{p-1}^i \varepsilon_0 T) - (\zeta_{p-1}^i \varepsilon_0 T)^p)) \\ &= \exp(-\pi \zeta_{p-1}^i \varepsilon_0^p (T^p - e_0 T)), \end{aligned}$$

where $\zeta_{p-1} := \zeta^{4g/(p-1)}$ is a $(p-1)$ -st root of unity. We take a positive integer s such that

$$\zeta + s \equiv 0 \pmod{\wp}.$$

Recall that we have defined an automorphism \bar{r} of $H(K)$ in §3.7 by $\bar{r}(h(T)) = h(\zeta T)$.

Proposition 4.4. *(1) For all $0 \leq i \leq p-2$, there exist $h_A^{(i)}, h_A'^{(i)} \in \bar{A} \cap \Gamma(K)$ and $h_-^{(i)}, h_-'^{(i)} \in \Gamma_-(K)$ such that*

$$(h^{(i)})^p = h_A^{(i)} h_-^{(i)}, \quad \bar{r}(h^{(i)})(h^{(i)})^s = h_A'^{(i)} h_-'^{(i)}.$$

(2) Let $0 \leq i < j \leq p-2$, and choose a positive integer t such that $\zeta_{p-1}^{j-i} \equiv t (\not\equiv 1) \pmod{\wp}$. Then, there exist $k_A^{(ij)} \in \bar{A} \cap \Gamma(K)$ and $k_-^{(ij)} \in \Gamma_-(K)$ such that

$$h^{(j)}(h^{(i)})^{-t} = k_A^{(ij)} k_-^{(ij)}.$$

Proof. (1) We may suppose $i = 0$ and will omit the suffix $^{(i)}$, so that $h(T) = h^{(0)}(T)$ for instance. From the equation (4.1), we have

$$\begin{aligned} h(T)^p &= \exp(-p\pi\varepsilon_0^p(T^p - e_0T)) \\ &= \exp(-p\pi\varepsilon_0^p a(T)) \cdot \exp(-p\pi\varepsilon_0^p g(T)). \end{aligned}$$

Since $a(T) \in A \cap \mathbb{Z}[[T^{-1}]] [T]$ and $g(T) \in T^{-1}\mathbb{Z}[[T^{-1}]]$, we have

$$\begin{aligned} h_A &:= \exp(-p\pi\varepsilon_0^p a(T)) \in \bar{A} \cap \Gamma(K) \\ h_- &:= \exp(-p\pi\varepsilon_0^p g(T)) \in \Gamma_-(K), \end{aligned}$$

hence the first claim is proved.

From the equation (4.1) and $\zeta^p = \zeta$, we compute

$$\begin{aligned} h(\zeta T)h(T)^s &= \exp(-(\zeta + s)\pi\varepsilon_0^p(T^p - e_0T)) \\ &= \exp(-(\zeta + s)\pi\varepsilon_0^p a(T)) \cdot \exp(-(\zeta + s)\pi\varepsilon_0^p g(T)). \end{aligned}$$

By the assumption $\zeta + s \equiv 0 \pmod{\wp}$, we have

$$\begin{aligned} h'_A(T) &:= \exp(-(\zeta + s)\pi\varepsilon_0^p a(T)) \in \bar{A} \cap \Gamma(K) \\ h'_-(T) &:= \exp(-(\zeta + s)\pi\varepsilon_0^p g(T)) \in \Gamma_-(K), \end{aligned}$$

and we are done.

(2) Put $\delta = \zeta_{p-1}^{j-i} - t \in \wp$. Then we have

$$h^{(j)}(h^{(i)})^{-t} = \exp(-\pi\delta\zeta_{p-1}^i\varepsilon_0^p(T^p - e_0T)).$$

The rest of the proof is the same as (1). □

4.4. Construction of p -torsion elements. Recall that we have constructed Dwork loops $h^{(i)}$ in §4.3.

Proposition 4.5. (1) We have $\{[h^{(i)}(\mathcal{O}_X, N)] \mid 0 \leq i \leq p-2\} = J[p]^\times \setminus \{0\}$.

(2) We have $J[p]^\times \cap \Theta = \{0\}$.

Proof. We fix i and put $h = h^{(i)}$, $(\mathcal{L}, \sigma) := h(\mathcal{O}_X, N) \in \text{Kr}(X, N)$. We first show $\mathcal{L} \in J \setminus \Theta$. By Proposition 2.3 (1), we have $\deg(\mathcal{L}) = 0$. The result of §3.4 shows that $(\mathcal{O}_X, N) \in \text{Kr}_{\text{an}}^0(X, N)$ satisfies the assumptions (A1) and (A2) of Theorem 2.4. It follows that $\mathcal{L} \notin \Theta$. In particular we get $\mathcal{L} \neq 0$.

In order to prove $\mathcal{L} \in J[p]^\times$, it suffices to show $\mathcal{L}^{\otimes p} = r^*\mathcal{L} \otimes \mathcal{L}^{\otimes s} = \mathcal{O}_X$, where $s \in \mathbb{Z}$ is the integer used in Proposition 4.4. For K -subspaces V_1, \dots, V_m of $H(K)$, we write $V_1 \cdot \dots \cdot V_m$ for the K -span of $\{\prod_{j=1}^m u_j \mid u_j \in V_j\}$. When $V = V_1 = \dots = V_m$ we write $V^m := V \cdot \dots \cdot V$. Let $V = \bar{W}(\mathcal{L}, \sigma)$. Proposition 2.3 shows that $V = h\bar{A}$. Thus $V^p = h^p\bar{A}$. By Proposition 2.2 and §2.5, we have $(\mathcal{L}, \sigma)^{\otimes p} = h^p(\mathcal{O}_X, N)$. Propositions

4.4 (1) and 2.3 show $[h^p(\mathcal{O}_X, N)] = [(\mathcal{O}_X, N)]$. We conclude $\mathcal{L}^{\otimes p} = \mathcal{O}_X$. Similarly, we have $r^*(V) \cdot V^s = \bar{r}(h)h^s\bar{A}$. By Proposition 2.2 and §2.5, we have $r^*(\mathcal{L}, \sigma) \otimes (\mathcal{L}, \sigma)^{\otimes s} = \bar{r}(h)h^s(\mathcal{O}_X, N)$. Now Propositions 4.4 (1) and 2.3 show $[\bar{r}(h)h^s(\mathcal{O}_X, N)] = [(\mathcal{O}_X, N)]$. We conclude $r^*(\mathcal{L}) \otimes \mathcal{L}^{\otimes s} = \mathcal{O}_X$.

It remains to show $[h^{(i)}(\mathcal{O}_X, N)] \neq [h^{(j)}(\mathcal{O}_X, N)]$ for $0 \leq i < j \leq p-2$. Propositions 4.4 (2) and 2.3 show that $[h^{(j)}(\mathcal{O}_X, N)] = [h^{(i)}(\mathcal{O}_X, N)^{\otimes t}]$ for some integer $t \not\equiv 1 \pmod{p}$. Since we have already seen that $[h^{(i)}(\mathcal{O}_X, N)]$ is a non-trivial element of $J[p]$, this completes the proof. \square

4.5. Proof of Theorem 1.1. We may suppose K is a finite extension of \mathbb{Q}_p satisfying the conditions stated at the beginning of this section. By Remark 4.2, we may also assume $i = 1$. Take $\mathcal{L} \in J[2]$ and $\mathcal{L}' \in J[p]^\times \setminus \{0\}$. We need to show $\mathcal{L} \otimes \mathcal{L}' \notin \Theta$. By Proposition 4.5, there exists a Dwork loop h such that $\mathcal{L}' = [h(\mathcal{O}_X, N)]$. By §3.5, there exists an N -trivialization σ of \mathcal{L} such that $W(\mathcal{L}, \sigma)$ admits an admissible basis $\{w_i\}$ satisfying $w_i \in \mathbb{Z}[[T^{-1}]]\langle T \rangle$ for all i . Hence (\mathcal{L}, σ) belongs to $\text{Kr}_{\text{an}}^0(X, N)$ and satisfies the assumptions (A1) and (A2) of Theorem 2.4. It follows that $[h(\mathcal{L}, \sigma)] \notin \Theta$. By Propositions 2.2, 2.3 and §2.5, we have $[h(\mathcal{L}, \sigma)] = [(\mathcal{L}, \sigma)] \otimes [h(\mathcal{O}_X, N)] = \mathcal{L} \otimes \mathcal{L}'$.

4.6. Proof of Theorem 1.2. We may assume Q is a non-Weierstrass point by Theorem 1.1. Then the same proof as the previous subsection works if we put §3.6 in the place of §3.5.

5. APPENDIX: SATO GRASSMANNIAN

In this section, we explain Anderson's theory [1] in a style much closer to his original framework. It will be apparent that the results in §2 are the same result stated in another way.

5.1. Sato Grassmannian. We work under the notation and assumption in §2.1. The *Sato Grassmannian* $\text{Gr}^{\text{alg}}(K)$ is the set of all K -subspace $V \subset K((T^{-1}))$ such that the K -dimensions of the kernel and cokernel of the map

$$f_V : V \rightarrow K((T^{-1}))/K[[T^{-1}]] ; v \mapsto v + K[[T^{-1}]]$$

are finite. The *index* of $V \in \text{Gr}^{\text{alg}}(K)$ is defined by

$$i(V) := \dim_K \text{Ker}(f_V) - \dim_K \text{Coker}(f_V).$$

Recall that $A := W(\mathcal{O}_X, N)$ is a K -subalgebra of $K((T^{-1}))$. For $V \in \text{Gr}^{\text{alg}}(K)$, we set $A_V := \{f \in K((T^{-1})) \mid fV \subset V\}$, which is a K -subalgebra of $K((T^{-1}))$. We define

$$\text{Gr}_A^{\text{alg}}(K) := \{V \in \text{Gr}^{\text{alg}}(K) \mid A_V = A\}.$$

For $V, V' \in \text{Gr}_A^{\text{alg}}(K)$, we define their product to be $V \cdot V' = \langle ww' \mid w \in V, w' \in V' \rangle_K$, under which $\text{Gr}_A^{\text{alg}}(K)$ becomes an abelian group.

Proposition 5.1 ([1, §2.3]; see also [9]). *The construction of §2.3 defines an isomorphism of abelian groups*

$$W : \text{Kr}(X, N) \rightarrow \text{Gr}_A^{\text{alg}}(K); \quad (\mathcal{L}, \sigma) \mapsto W(\mathcal{L}, \sigma)$$

which satisfies the following properties:

- (1) We have $i(W(\mathcal{L}, \sigma)) = \deg(\mathcal{L}) + 1 - g$ for any $(\mathcal{L}, \sigma) \in \text{Kr}(X, N)$.
- (2) For $V, V' \in \text{Gr}_A^{\text{alg}}(K)$, one has $[W^{-1}(V)] = [W^{-1}(V')]$ if and only if $V = uV'$ for some $u \in K[[T^{-1}]]^*$.

All results in §2.1-2.5 are explained by this proposition.

5.2. p -adic Sato Grassmannian. Now we use the assumption and notation of §2.8. Let $H_+(K)$ and $H_-(K)$ be the closed K -subspaces of $H(K)$ defined by

$$H_+(K) := \left\{ \sum_i a_i T^i \in H(K) \mid a_i = 0 \text{ (for all } i \leq 0) \right\},$$

$$H_-(K) := \left\{ \sum_i a_i T^i \in H(K) \mid a_i = 0 \text{ (for all } i > 0) \right\}.$$

The p -adic Grassmannian $\text{Gr}^{\text{an}}(K)$ is the set of all K -subspaces $\bar{V} \subset H(K)$ such that \bar{V} is the image of a K -linear injective map $w : H_+(K) \rightarrow H(K)$ satisfying the following conditions: there exist an integer i_0 , a K -linear operator $v : H_+(K) \rightarrow H_-(K)$ with $\|v\| \leq 1$, and a K -linear endomorphism u on $H_+(K)$ with $\|u\| \leq 1$ that is a uniform limit of bounded K -linear operators of finite rank (i.e. *completely continuous*), such that the map $T^{i_0}w$ has the form

$$T^{i_0}w = \begin{bmatrix} 1 + u \\ v \end{bmatrix} : H_+(K) \rightarrow \begin{bmatrix} H_+(K) \\ H_-(K) \end{bmatrix}.$$

The *index* of $\bar{V} \in \text{Gr}^{\text{an}}(K)$, denoted by $i(\bar{V})$, is defined by the difference of the dimensions of the kernel and cokernel of the projection map $\bar{V} \rightarrow H_+(K)$.

Proposition 5.2 ([1, §3.2]). *There is an injective map*

$$\text{Gr}^{\text{an}}(K) \hookrightarrow \text{Gr}^{\text{alg}}(K), \quad \bar{V} \mapsto \bar{V}^{\text{alg}} := \bar{V} \cap K((T^{-1})).$$

For any $\bar{V} \in \text{Gr}^{\text{an}}(K)$, one has $i(\bar{V}) = i(\bar{V}^{\text{alg}})$. For $V \in \text{Gr}^{\text{alg}}(K)$, there exists $\bar{V} \in \text{Gr}^{\text{an}}(K)$ such that $\bar{V}^{\text{alg}} = V$ if and only if V has an admissible basis $\{w_i\}$ such that $w_i \in H(K)$ for all i and $\|w_i\| = 1$ for almost all i .

By this proposition, we regard $\text{Gr}^{\text{an}}(K)$ as a subset of $\text{Gr}^{\text{alg}}(K)$. It follows that $\text{Kr}_{\text{an}}(X, N) = \{(\mathcal{L}, \sigma) \in \text{Kr}(X, N) \mid W(\mathcal{L}, \sigma) \in \text{Gr}^{\text{an}}(K)\}$.

5.3. **Action of p -adic loop group and Anderson’s theorem.** In [1, §3.3], the action

$$\Gamma(K) \times \mathrm{Gr}^{\mathrm{an}}(K) \rightarrow \mathrm{Gr}^{\mathrm{an}}(K), \quad (h, \bar{V}) \mapsto h\bar{V} := \{hv \mid v \in \bar{V}\}$$

of $\Gamma(K)$ on $\mathrm{Gr}^{\mathrm{an}}(K)$ is defined. Proposition 2.3 is also proved in loc. cit.

Finally, Theorem 2.4 is a reformulation of [1, Lemma 3.5.1]. Anderson proved this extraordinary result by introducing the p -adic version of *Sato tau-function*, which plays a central role in Sato’s theory of KP hierarchy (see [12–14]).

Acknowledgement. We would like to express our gratitude to Noriyuki Otsubo for his insightful comments. In particular, the remark in §3.8 is suggested by him. We are also deeply grateful to Takeshi Ikeda for stimulating discussion. We learned the importance of the equation of the form (4.1) from him .

REFERENCES

- [1] G. W. Anderson, *Torsion points on Jacobians of quotients of Fermat curves and p -adic soliton theory*, Invent. Math. **118** (1994), no. 3, 475–492.
- [2] N. Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves*, Amer. J. Math. **113** (1991), no. 5, 779–833.
- [3] J. Boxall and D. Grant, *Examples of torsion points on genus two curves*, Trans. Amer. Math. Soc. **352** (2000), no. 10, 4533–4555.
- [4] R. F. Coleman, *Torsion points on curves and p -adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168.
- [5] B. Dwork, *On the zeta function of a hypersurface*, Publications Mathématiques de l’IHÉS **12** (1962), no. 1, 5–68.
- [6] D. Grant, *Torsion on theta divisors of hyperelliptic Fermat Jacobians*, Compos. Math. **140** (2004), no. 6, 1432–1438.
- [7] N. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. **30** (1978), no. 6, 1183–1205.
- [8] N. Koblitz, *p -adic analysis: A short course on recent work*, Vol. 46, Cambridge Univ Pr, 1980.
- [9] D. Mumford, *An algebro-geometric construction of commuting operators and of solutions to the Toda lattice equation, Korteweg de Vries equation and related nonlinear equation*, Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977), 1978, pp. 115–153.
- [10] ———, *Tata lectures on theta. II*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.
- [11] M. Raynaud, *Sous-variétés d’une variété abélienne et points de torsion*, Arithmetic and geometry, Vol. I, 1983, pp. 327–352.
- [12] M. Sato and Y. Sato, *Soliton equations as dynamical systems on infinite-dimensional Grassmann manifold*, Nonlinear partial differential equations in applied science (Tokyo, 1982), 1983, pp. 259–271.
- [13] M. Sato, *The KP hierarchy and infinite-dimensional Grassmann manifolds*, Theta functions—Bowdoin 1987, Part 1 (Brunswick, ME, 1987), 1989, pp. 51–66.
- [14] G. Segal and G. Wilson, *Loop groups and equations of KdV type*, Inst. Hautes Études Sci. Publ. Math. (1985), no. 61, 5–65.

- [15] P. Tzermias, *The Manin-Mumford conjecture: a brief survey*, Bull. London Math. Soc. **32** (2000), no. 6, 641–652.

MATHEMATICAL INSTITUTE, TOHOKU UNIVERSITY, SENDAI 980-8578, JAPAN

E-mail address, Takao Yamazaki: ytakao@math.tohoku.ac.jp

E-mail address, Yuken Miyasaka: sa7m27@math.tohoku.ac.jp